

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-301857

(43)Date of publication of application : 13.11.1998

(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 09-123504

(71)Applicant : NEC CORP

(22)Date of filing : 25.04.1997

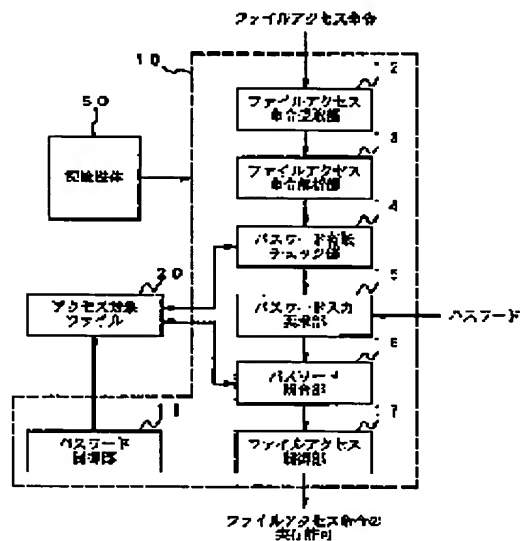
(72)Inventor : MATSUI SHINICHI

(54) FILE SECURITY PROTECTING CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a file security protecting device capable of protecting the security of confidential data stored in an easily attachable/detachable storage medium and permitting access to non-confidential data stored in the storage medium to a user who does not deal with the confidential data.

SOLUTION: This circuit is provided with a file access instruction analyzing part 13 which analyzes an access instruction, and specifies a data file being the object of access, password input requesting part 15 which requests the input of a password when the data file specified by the file access instruction analyzing part 13 is a data file whose password is set, password collating part 16 which judges whether or not a password inputted in response to the request of the password input requesting part 15 is legal, and file access controlling part 17 which permits the execution of an access instruction to an operating a system when it is judged that the input password is legal by the password collating part 16.



LEGAL STATUS

[Date of request for examination] 25.04.1997

[Date of sending the examiner's decision of rejection] 17.10.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-301857

(43) 公開日 平成10年(1998)11月13日

(51) Int.Cl.⁶

G 0 6 F 12/14
12/00

識別記号

3 2 0
5 3 7

F I

G 0 6 F 12/14
12/00

3 2 0 C
5 3 7 D

審査請求 有 請求項の数 4 F D (全 6 頁)

(21) 出願番号 特願平9-123504

(22) 出願日 平成9年(1997)4月25日

(71) 出願人 000004237

日本電気株式会社
東京都港区芝五丁目7番1号

(72) 発明者 松井 伸一

東京都港区芝五丁目7番1号 日本電気株
式会社内

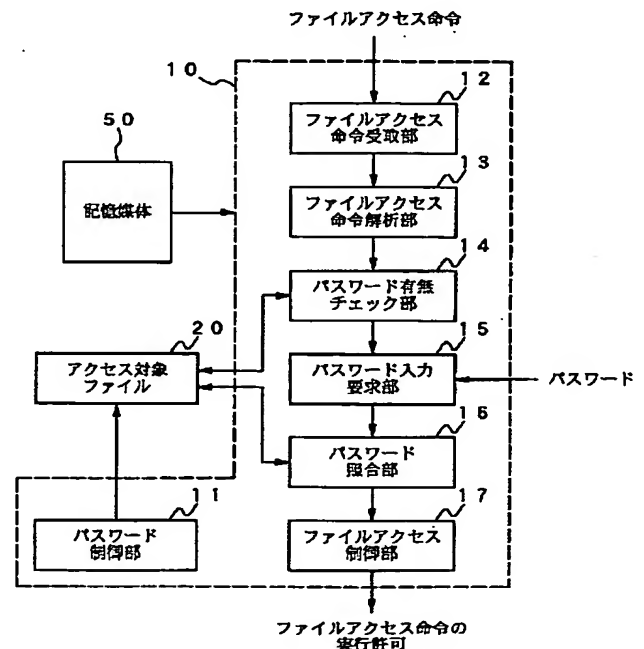
(74) 代理人 弁理士 松本 正夫

(54) 【発明の名称】 ファイル機密保護装置

(57) 【要約】

【課題】 着脱が容易な記憶媒体に格納された機密データの機密性を保護すると共に、機密データを扱わない利用者に対して当該記憶媒体に格納された非機密データへのアクセスを許可するファイル機密保護装置を提供する。

【解決手段】 アクセス命令を解析してアクセス対象のデータファイルを特定するファイルアクセス命令解析部13と、ファイルアクセス命令解析部13により特定されたデータファイルが、パスワードを設定されたデータファイルである場合に、当該パスワードの入力を要求するパスワード入力要求部15と、パスワード入力要求部15の要求に応じて入力されたパスワードが正しいかどうかを判断するパスワード照合部16と、パスワード照合部16により入力パスワードが正当と判断された場合に、オペレーティングシステムに対して前記アクセス命令の実行を許可するファイルアクセス制御部17とを備える。



【特許請求の範囲】

【請求項1】 オペレーティングシステムによるデータファイルへのアクセス命令の実行を許可するかどうかを制御することにより、前記データファイルに格納された機密データの機密性を保護するファイル機密保護装置において、

外部から入力された前記アクセス命令を解析してアクセス対象のデータファイルを特定するアクセス命令解析手段と、

前記アクセス命令解析手段により特定されたデータファイルが、パスワードを設定されたデータファイルである場合に、当該パスワードの入力を要求するパスワード要求手段と、

前記パスワード要求手段の要求に応じて入力されたパスワードが正当かどうかを判断する照合手段と、

前記照合手段により入力パスワードが正当と判断された場合に、前記オペレーティングシステムに対して前記アクセス命令の実行を許可するアクセス制御手段とを備えることを特徴とするファイル機密保護装置。

【請求項2】 データファイルに対して、パスワードを設定するパスワード制御手段をさらに備えることを特徴とする請求項1に記載のファイル機密保護装置。

【請求項3】 データファイルに対して、パスワードを新規に設定すると共に、既にデータファイルに設定されているパスワードを変更し、または削除するパスワード制御手段をさらに備えることを特徴とする請求項1に記載のファイル機密保護装置。

【請求項4】 前記パスワード制御手段が、前記データファイルに格納されるデータの一部として前記パスワードを設定することを特徴とする請求項2または請求項3に記載のファイル機密保護装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、パーソナルコンピュータクラスのコンピュータのオペレーティングシステム上で実行されるファイルアクセス命令に対するデータファイルの機密保護装置に関し、特にフロッピーディスクその他の着脱の容易な記憶媒体に格納されたデータファイルの機密を保護するファイル機密保護装置に関する。

【0002】

【従来の技術】 コンピュータシステムで用いられるデータファイルにおいて、個人の情報が含まれるデータファイルのように、不特定の第三者によって自由に参照、更新、削除されることを防止する必要がある場合がある。そのため、従来から、特定のデータファイルの機密を保護すべく、ファイルアクセスの正当性をチェックする手段が提案されている。この種の従来技術として、特開平4-171554号公報に開示されたファイル機密保護装置や特開平3-91047号公報に開示された情報処

理システムがある。

【0003】 特開平4-171554号公報には、機密保護の対象ファイルのファイル名とパスワードとを対応させて記録したパスワード管理ファイルを備え、該パスワード管理ファイルに登録された対象ファイルに対するファイルアクセス命令を受け取った場合に、当該ファイルアクセス命令によりアクセスしようとするファイルに対するパスワードの入力を要求し、入力されたパスワードと当該ファイルに対応付けられたパスワードとを照合し、両パスワードが一致した場合にのみ当該ファイルアクセス命令をオペレーティングシステムに送ることにより、前記パスワード管理ファイルに登録されたファイルの機密を保護するファイル機密保護装置について記載されている。

【0004】 しかし、前記パスワード管理ファイルに、フロッピーディスクや光磁気ディスクその他の容易に着脱可能な記憶媒体に格納したファイルを常時的確に登録しておくことは困難である。したがって、前記パスワード管理ファイルを用いた機密保護手段では、前記着脱の容易な記憶媒体に格納したファイルに対する十分な機密保護を実現することはできなかった。

【0005】 また、特開平3-91047号公報には、情報処理装置（コンピュータ）と補助記憶装置とを備え、前記情報処理装置を利用可能なユーザに関する所定の情報を格納する記憶手段を前記補助記憶装置と前記情報処理装置とに設け、前記補助記憶装置の記憶手段に記憶してある情報と前記情報処理装置の記憶手段に記憶してある情報とを照合し、双方が一致しない場合には前記補助記憶装置へのアクセスを禁止する手段を前記情報処理装置に設けた情報処理システムについて記載されている。

【0006】 しかし、この場合、前記補助記憶装置における記憶媒体単位でパスワードが設定されるため、1個の記憶媒体に機密データと非機密データとが存在する場合、機密データを扱わない利用者は、当該記憶媒体に格納されている非機密データを利用することができなかった。

【0007】

【発明が解決しようとする課題】 上述したように、従来のデータファイルの機密保護装置によれば、ファイル単位でアクセスの可否を制御する場合には、着脱が容易な記憶媒体に格納されたデータファイルに対するアクセスの可否を制御することができないという欠点があった。

【0008】 また、記憶媒体単位でアクセスの可否を制御すると、機密データを扱わない利用者が当該記憶媒体に格納されている非機密データにアクセスできないという欠点があった。

【0009】 本発明の目的は、機密データと非機密データとを格納した着脱が容易な記憶媒体を複数の利用者にて使用する場合に、記憶媒体に格納された機密データの

漏洩や改変を防止すると共に、機密データを扱わない利用者に対して当該記憶媒体に格納された非機密データへのアクセスを許可することを可能としたファイル機密保護装置を提供することである。

【0010】

【課題を解決するための手段】上記の目的を達成する本発明のファイル機密保護装置は、オペレーティングシステムによるデータファイルへのアクセス命令の実行を許可するかどうかを制御することにより、前記データファイルに格納された機密データの機密性を保護するファイル機密保護装置において、外部から入力された前記アクセス命令を解析してアクセス対象のデータファイルを特定するアクセス命令解析手段と、前記アクセス命令解析手段により特定されたデータファイルが、パスワードを設定されたデータファイルである場合に、当該パスワードの入力を要求するパスワード要求手段と、前記パスワード要求手段の要求に応じて入力されたパスワードが正当かどうかを判断する照合手段と、前記照合手段により入力パスワードが正当と判断された場合に、前記オペレーティングシステムに対して前記アクセス命令の実行を許可するアクセス制御手段とを備えることを特徴とする。

【0011】請求項2の本発明のファイル機密保護装置は、データファイルに対して、パスワードを設定するパスワード制御手段をさらに備えることを特徴とする。

【0012】請求項3の本発明のファイル機密保護装置は、データファイルに対して、パスワードを新規に設定すると共に、既にデータファイルに設定されているパスワードを変更し、または削除するパスワード制御手段をさらに備えることを特徴とする。

【0013】請求項4の本発明のファイル機密保護装置は、前記パスワード制御手段が、前記データファイルに格納されるデータの一部として前記パスワードを設定することを特徴とする。

【0014】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0015】図1は、本発明の一実施形態によるファイル機密保護装置の構成を示すブロック図である。図2は、本実施形態のファイル機密保護装置を搭載したコンピュータシステムの構成例を示す概略図である。

【0016】図2に示すように、本実施形態のファイル機密保護装置10は、アプリケーションプログラム(AP)30とオペレーティングシステム(OS)40との間に位置する。そして、アプリケーションプログラム30からのアクセス対象ファイル20へのアクセス命令がオペレーティングシステム40にわたる前に、当該アクセス命令をチェックし、機密データへのアクセスの可否を制御する。

【0017】図1に示すように、本実施形態のファイル

機密保護装置10は、アクセス対象ファイル20に対してパスワードの設定、変更、削除を行うパスワード制御部11と、ファイルアクセス命令を受け取り、アクセス対象ファイル20を参照してファイル機密保護機能を実現するファイルアクセス命令受取部12、ファイルアクセス命令解析部13、パスワード有無チェック部14、パスワード入力要求部15、パスワード照合部16、およびファイルアクセス制御部17とを備える。なお、図1には本実施形態における特徴的な構成のみを記載し、他の一般的な構成については記載を省略してある。

【0018】本実施形態の各構成は、コンピュータプログラムで制御されたCPUとRAMその他の内部メモリとで実現される。CPUを制御するコンピュータプログラムは、図1に示す記憶媒体50に格納されて提供される。記憶媒体50は、磁気ディスクや半導体メモリその他の一般的な記憶媒体である。記憶媒体50から所定の読取手段を経てコンピュータプログラムをロードすることにより、CPUにて、上述したパスワード制御部11、ファイルアクセス命令受取部12、ファイルアクセス命令解析部13、パスワード有無チェック部14、パスワード入力要求部15、パスワード照合部16、およびファイルアクセス制御部17の各機能実行部が実現される。

【0019】アクセス対象ファイル20は、任意の補助記憶装置に格納されている。補助記憶装置の記憶媒体としては、フロッピーディスクや光磁気ディスクその他の着脱が容易な記憶媒体を含む。また、アクセス対象ファイル20には、図2に示すように、標準的に、ファイル名21と、ファイル名21に対応するデータ23とが格納されている。データ23は、通常、複数のレコードに分割されて格納されている。ファイル名21にはデータ23が格納されたレコードの先頭のアドレス22が付加され、各レコードのデータには当該データの続きが格納されたレコードを示すアドレス24が付加されている。当該データが当該ファイル名21に対応するデータ23の最後である場合、続きのデータのアドレスに変えてデータ23の絡端であることを示す記号が付加される。

【0020】アクセス対象ファイル20に対して、アクセスできる利用者を制限するためのパスワードを設定する場合、図2に示すように、ファイル名21に、アドレス22の代わりに、パスワード26を格納したレコードのアドレス25を付加する。そして、パスワード26に、データ23が格納されたレコードの先頭のアドレス22を付加する。

【0021】パスワード制御部11は、任意のアクセス対象ファイル20に対して新規にパスワードを設定する場合や、設定されているパスワードを変更または削除する場合に、1つのコマンドとして起動される。パスワード制御部11が起動したならば、利用者は、新規設定、更新、削除の動作モードの中から1つを選択する。新規

設定を選択した場合は、設定するファイル名とパスワードを入力することにより、当該アクセス対象ファイル20に対してパスワード26が登録される。すなわち、ファイル名21に付加されたアドレスを、当該パスワードを格納したレコードのアドレスに変更し、パスワード26に、データ23が格納されたレコードの先頭のアドレス22を付加する。これ以後、当該アクセス対象ファイル20は、設定されたパスワードを入力しない限りアクセスすることができない。

【0022】動作モードとして変更を選択した場合は、パスワードを変更しようとするファイル名と旧いパスワードと変更後の新しいパスワードとを入力することにより、当該アクセス対象ファイル20のパスワード26が更新される。これ以後、当該アクセス対象ファイル20は、更新された新しいパスワードを入力しない限りアクセスすることができない。

【0023】動作モードとして削除を選択した場合は、パスワードを削除しようとするファイル名とパスワードとを入力することにより、当該アクセス対象ファイル20に設定されていたパスワード26が削除される。すなわち、パスワード26を格納したレコードを消去し、ファイル名21に付加されたパスワードを格納していたレコードのアドレス25がデータ23を格納するレコードの先頭のアドレス24に変更される。これ以後、当該アクセス対象ファイル20は、パスワードなしでアクセスできることとなる。

【0024】ファイルアクセス命令受取部12は、アプリケーションプログラム30から発行されたアクセス対象ファイル20へのアクセス命令を入力し、バッファにセーブする。

【0025】ファイルアクセス命令解析部13は、ファイルアクセス命令受取部12によってバッファにセーブされたファイルアクセス命令の種類（例えば、ファイル作成、読み取り、更新、削除）とアクセス対象ファイル20のファイル名とを解析する。

【0026】パスワード有無チェック部14は、ファイルアクセス命令解析部13による解析結果に基づいてアクセス対象ファイル20を参照し、ファイル名に付加されたアドレスを検索して、当該アドレスのレコードに格納されたデータがパスワードかどうかを確認する。パスワードである場合はパスワード入力要求部15に制御を渡し、パスワードでない場合は当該ファイルアクセス命令をオペレーティングシステム40に転送する。

【0027】パスワード入力要求部15は、ファイルアクセス命令が正当なものか否かを判断するため、パスワードの入力要求を行い、入力されたパスワードを専用のバッファにセーブする。パスワードの入力要求は、例えば、ディスプレイ装置にパスワードの入力を要求するメッセージを表示したり、音声により利用者に通知したりすることにより行う。パスワードの入力は、キーボード

その他の入力デバイスを用いて行う。

【0028】パスワード照合部16は、パスワード入力要求部15により専用バッファにセーブされたパスワードとアクセスしようとするアクセス対象ファイル20に登録されているパスワード26とを照合する。

【0029】ファイルアクセス制御部17は、パスワード照合部16によるパスワードの照合結果においてパスワードが一致した場合に、ファイルアクセス命令の実行を許可し、ファイルアクセス命令受取部12で受け取ってバッファにセーブされたファイルアクセス命令をオペレーティングシステム40に転送して実行させる。一方、パスワードが一致しなかった場合は、エラーメッセージ出力命令を発行してオペレーティングシステム40に送り、利用者に対してエラーメッセージを通知する。エラーメッセージの通知は、ディスプレイ装置への表示や音声により行う。なお、実行を許可したファイルアクセス命令が当該アクセス対象ファイル20を削除するのであれば、当該アクセス対象ファイル20のパスワード26を格納したレコードも共に削除する。

【0030】次に、図3のフローチャートを参照して本実施例によるアクセス対象ファイルへのアクセス制御の動作について説明する。

【0031】まず、ファイルアクセス命令受取部12が、アプリケーションプログラム30から発行されたファイルアクセス命令を受け取ると（ステップ301）、ファイルアクセス命令解析部13が、当該ファイルアクセス命令を解析する（ステップ302）。

【0032】次に、パスワード有無チェック部14が、ファイルアクセス命令解析部13による解析結果に基づいて、アクセスしようとするアクセス対象ファイル20を参照し、パスワードが設定されているかどうかを確認する（ステップ303）。パスワードが設定されていない場合は、当該アクセス対象ファイル20はアクセス可能な利用者を制限していないので、オペレーティングシステム40に当該ファイルアクセス命令を送り、当該アクセス対象ファイル20へのアクセスを実行させる（ステップ304、309）。

【0033】一方、パスワードが設定されているならば、パスワード入力要求部15によるパスワード入力要求処理に移行する（ステップ304、305）。パスワードが入力されたならば、パスワード照合部16がアクセス対象ファイル20を参照し、パスワードの照合を行って、入力されたパスワードが正当かどうかを判断する（ステップ306、307）。入力されたパスワードが正当であれば、当該アクセス対象ファイル20へのアクセスが許可されているため、オペレーティングシステム40に当該ファイルアクセス命令を送り、当該アクセス対象ファイル20へのアクセスを実行させる（ステップ308、309）。

【0034】入力されたパスワードが不正である場合

は、エラーメッセージを出力して処理を終了する（ステップ308、310）。

【0035】次に、パスワードを付加したアクセス対象ファイルを着脱可能な記憶媒体に格納した場合のアクセス制御の動作について説明する。

【0036】上述したように、アクセスを許可するためのパスワードは、アクセス対象ファイル20自体に登録されるため、アクセス対象ファイル20が格納されている記憶媒体の種類は何ら問題とならない。したがって、本実施形態によるファイル機密保護装置を備えるコンピュータシステムでは、上述の通りの動作によりアクセス制御が行われる。

【0037】これに対し、本発明のファイル機密保護装置を有しないコンピュータシステムでは、上述したようなパスワードに基づくアクセス制御を行うことはできない。しかし、パスワードを付加したファイルを参照しようとした場合、ファイル名にはデータの先頭位置のアドレスの代わりにパスワードのアドレスが付加されており、パスワードもデータの一部とみなされることにより、データの配置がずれるため、データの内容を正しく参照することができない。このため、データを改変することもできない。

【0038】以上好ましい実施例をあげて本発明を説明したが、本発明は必ずしも上記実施例に限定されるものではない。

【0039】

【発明の効果】以上詳細に説明したように、本発明のファイル機密保護装置は、アクセス対象となるファイル自体に当該ファイルへのアクセスを制限するパスワードを格納したため、当該ファイルが格納された記憶媒体の種類に関わらず、アクセスの可否に関する制御を行うことができる。これにより、フロッピーディスクや光磁気ディスクと行った着脱が容易な記憶媒体に格納されたファイルに対しても有効なアクセス制限を行うことができ、機密データを格納することができるという効果がある。

【0040】また、パスワードをファイル単位で設定できるため、着脱が容易な記憶媒体に格納されたファイル

にパスワードを設定した場合であっても、当該記憶媒体中に機密データと非機密データとを混在させることができる。これにより、当該記憶媒体を複数の利用者にて使用する場合に、機密データを扱わない利用者が非機密データに対するアクセスできなくなるという不都合を回避できるという効果がある。

【0041】さらに、本発明で用いるパスワードは、当該ファイルのデータの一部として当該ファイルに格納されているため、着脱が容易な記憶媒体に格納されたファイルにパスワードを設定して機密データを格納し、本発明のファイル機密保護装置を有しないコンピュータシステムで当該記憶媒体を使用した場合、当該コンピュータシステムではパスワードを設定されたファイルに格納されているデータを正しく読み取ることができず、機密データの機密性が維持される。これにより、確実に機密データの保護ができるという効果がある。

【図面の簡単な説明】

【図1】 本発明の一実施形態によるファイル機密保護装置の構成を示すブロック図である。

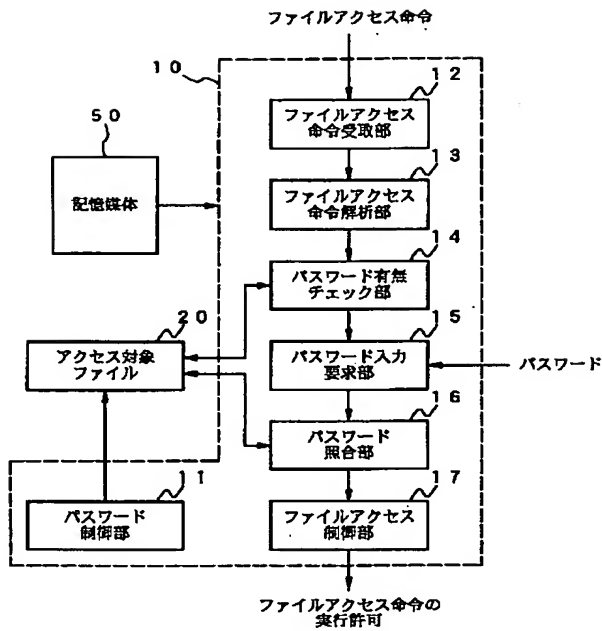
【図2】 本実施形態のファイル機密保護装置を搭載したコンピュータシステムの構成例を示す概略図である。

【図3】 本実施形態のファイル機密保護装置によるアクセス制御動作を示すフローチャートである。

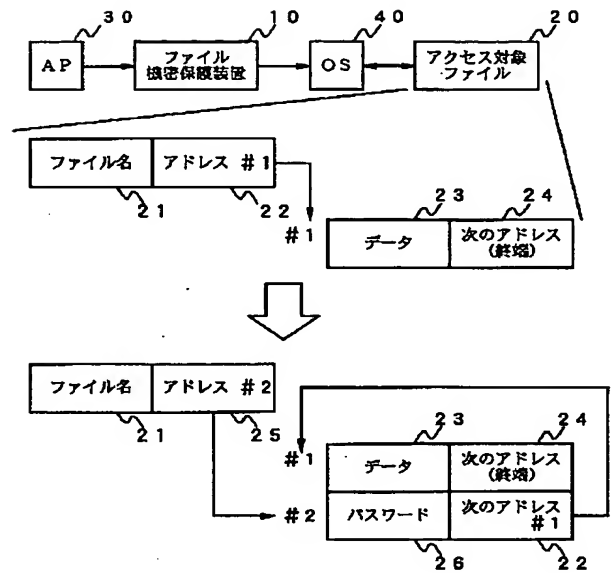
【符号の説明】

- 10 ファイル機密保護装置
- 11 パスワード制御部
- 12 ファイルアクセス命令受取部
- 13 ファイルアクセス命令解析部
- 14 パスワード有無チェック部
- 15 パスワード入力要求部
- 16 パスワード照合部
- 17 ファイルアクセス制御部
- 20 アクセス対象ファイル
- 30 アプリケーションプログラム
- 40 オペレーティングシステム
- 50 記憶媒体

【図1】



【図2】



【図3】

